REMARKS

Claims 14-21 are all the claims pending in the application.

I. Claim Rejections under 35 U.S.C. § 112, first paragraph

Claims 14-21 have been rejected under 35 U.S.C. § 112, first paragraph as failing to comply with the written description requirement. Applicants kindly request that the Examiner reconsider this rejection in view of the following comments.

Regarding claim 14, Applicants note that this claim recites the feature of "a digital signature management unit configured to (i) generate a hash value of the encrypted license information before the encrypted license information is stored into the storage unit, and store the generated hash value into a built-in memory, and (ii) read the encrypted license information stored in the storage unit, generate a hash value of the read encrypted license information, and compare the hash value stored in the built-in memory with the generated hash value of the read encrypted license information..." (it is noted that claims 20 and 21 recite similar features).

Applicants respectfully submit that the above-noted feature is supported by the specification for the following reasons.

(A) The specification describes, on page 14, lines 7-11, that it is possible to verify whether or not information stored in the secure flash unit is rewritten without permission, by comparing the information stored in the secure flash unit with information stored in the TRM unit (i.e., a copy of the information before the information is stored into the secure flash unit).

(B) The specification describes, on page 15, lines 15-17, another method for detecting rewriting without permission in which information may be stored in the secure flash unit and a hash value of the information may be held in the TRM unit.

(C) Applicants note that it can be derived from (A) and (B) that it is possible to verify whether or not the "information" stored in the secure flash unit is rewritten without permission by comparing a hash value generated from the information stored in the secure flash unit with a hash value of the information stored in the TRM unit (i.e., a hash value of the information before the information is stored into the secure flash unit).

(D) Further, the specification describes, on page 8, lines 23-25, that an encrypted license ticket is stored in the secure flash unit, and also describes, on page 15, lines 17-19, a hash value of the license ticket.

(E) With an assumption that the encrypted license ticket in (D) corresponds to the "information" in (C), Applicants note that it can be derived that it is possible to verify whether or not the encrypted license ticket stored in the secure flash unit is rewritten without permission by comparing a hash value generated from the encrypted license ticket stored in the secure flash unit with a hash value of the encrypted license ticket stored in the TRM unit (i.e., a hash value of the encrypted license ticket before the encrypted license ticket is stored into the secure flash unit).

Based on the foregoing comments, Applicants respectfully submit that specification provides support for the above-noted feature recited in claim 14 of "a digital signature management unit configured to (i) generate a hash value of the encrypted license information before the encrypted license information is stored into the storage unit, and store the generated hash value into a built-in memory, and (ii) read the encrypted license information stored in the storage unit, generate a hash value of the read encrypted license information, and compare the hash value stored in the built-in memory with the generated hash value of the read encrypted license information…", and also provides support for the corresponding features recited in claims 20 and 21.

Accordingly, Applicants respectfully submit that claims 14, 20 and 21, as well as dependent claims 15-19, satisfy the written description requirement of 35 U.S.C. 112, first paragraph. As such, Applicants kindly request that the above-noted rejection be reconsidered and withdrawn.

II. Claim Rejections under 35 U.S.C. § 103(a)

Claims 14-21 have been rejected under 35 U.S.C. § 103(a) as being unpatentable over Hori et al. (US 2002/0184154) in view of Ginter et al. (US 5,892,900). Applicants kindly request that the Examiner reconsider this rejection in view of the following comments.

A. Claims 14-19

Regarding claim 14 (which is an apparatus claim), Applicants note that in the Response to Amendment section of the Office Action (see item 3 on pages 2-7), the Examiner has indicated that the functional language recited in claim 14 has not been given patentable weight based on the language set forth in MPEP 2114 which indicates that claims directed to an apparatus must be distinguished in terms of structure rather than function.

Applicants respectfully disagree with the position being taken by the Examiner for the following reasons.

In particular, contrary to the assertion of the Examiner, Applicants respectfully submit that the functional language recited in the claims cannot simply be ignored. The MPEP, for example, specifically points out that there is nothing intrinsically wrong in defining something by what it does rather than by what it is (see MPEP §2173.05(g)). The MPEP further sets forth that "[a] functional limitation must be evaluated and considered, just like any other limitation of

the claim, for what it fairly conveys to a person of ordinary skill in the pertinent art in the context in which it is used" (see MPEP § 2173.05(g) (emphasis added).

In this regard, Applicants note that functional limitations of an apparatus claim require that the claimed apparatus include structure enabling it to perform the functional limitations. Thus, in order for a prior art reference to meet a functional limitation in an apparatus claim, the prior art structure must inherently be capable of performing that function.

For example, MPEP §2114, which was cited by the Examiner in the Office Action, provides evidence that a prior art structure must inherently be capable of performing the claimed function in order for the prior art structure to meet the claim limitation.

In particular, as specifically discussed in MPEP §2114, the Federal Circuit held in *In re Schreiber* (Applicants note that the Examiner has made reference to *In re Schreiber* on pages 3 and 4 of the Office Action) that the absence of disclosure in a prior art reference relating to function did not defeat the Board's finding of anticipation of a claimed apparatus because the limitations at issue were found to be inherent in the prior art reference. In other words, because the prior art structure in *Schreiber* was inherently capable of performing the claimed functional limitations, the Federal Circuit found that the prior art structure anticipated the claim in question.

The Examiner appears to recognize this point (i.e., that the prior art structure must be inherently capable of performing the claimed functional limitations) by stating on page 14 of the Office Action that "[i]f the prior art structure is capable of performing the intended use, then it meets the claim."

Applicants note out, however, that the Examiner has not followed this required course of analysis when formulating the rejection of claim 14. That is, the Examiner has not demonstrated that the structure in the cited prior art references is capable of performing the functional

limitations recited in claim 14. Instead, the Examiner has simply ignored the functional language in explicit contradiction to the guidelines set forth in the MPEP.

In this regard, Applicants respectfully submit that the structure in the cited prior art is not inherently capable of performing the functions recited in claim 14, and therefore, submit that cited prior art does not render claim 14 unpatentable.

For example, Applicants note that claim 14 recites the feature of a digital signature management unit configured to (i) generate a hash value of the encrypted license information before the encrypted license information is stored into the storage unit, and store the generated hash value into a built-in memory, and (ii) read the encrypted license information stored in the storage unit, generate a hash value of the read encrypted license information, and compare the hash value stored in the built-in memory with the generated hash value of the read encrypted license information, with a result of the comparison being used to verify validity of the read encrypted license information, the validity indicating that the read encrypted license information has not been tampered with.

Applicants respectfully submit that Hori and Ginter do not teach or suggest at least the above-noted feature recited in claim 14.

In particular, with respect to Hori, Applicants note that this reference discloses the use of a controller 1420 in a memory card 110, wherein the controller has the ability to generate a hash value, and to encrypt the generated hash value (see paragraph [0223]). In this regard, however, Applicants note that the hash value of Hori is merely a hash value of status information (i.e., information in which a status flag is added to a reception log) (see paragraphs [0219] through [0222]), and therefore, is clearly not a hash value of encrypted license information as recited in claim 14.

In addition, as explained in Hori, a decryption process is performed on the encrypted hash value to obtain a signature data hash corresponding to the encrypted data, and then authenticity of the status information is checked based on the encrypted status and the signature data (see paragraph [0027]). Thus, while Hori discloses the ability to determine the authenticity of the status information based on the encrypted status information and the signature data, Applicants respectfully submit that this aspect of Hori clearly does not correspond to the feature recited in amended claim 14 which indicates that the hash value stored in the built-in memory is compared with the generated hash value of the read encrypted license information.

Based on the foregoing, Applicants note that while Hori discloses the ability to generate a hash value of status information, and to determine the authenticity of the status information based on the encrypted status information and the signature data, that Hori does not disclose or in any way suggest the above-noted feature recited in claim 14 of a digital signature management unit configured to (i) generate a hash value of the encrypted license information before the encrypted license information is stored into the storage unit, and store the generated hash value into a built-in memory, and (ii) read the encrypted license information stored in the storage unit, generate a hash value of the read encrypted license information, and compare the hash value stored in the built-in memory with the generated hash value of the read encrypted license information, with a result of the comparison being used to verify validity of the read encrypted license information, the validity indicating that the read encrypted license information has not been tampered with.

Further, Applicants respectfully submit that Ginter fails to cure the above-noted deficiencies of Hori. Accordingly, Applicants respectfully submit that claim 14 is patentable over the cited prior art, an indication of which is kindly requested.

To the extent that the Examiner attempts to take the position that the structure described in the cited prior art is inherently capable of performing the claimed functions set forth in claim 14, Applicants note that the "fact that a certain result or characteristic may occur or be present in the prior art is not sufficient to establish the inherency of that result or characteristic." See MPEP 2112 (IV)(emphasis in original). When "relying on a theory of inherency, the examiner must provide a basis in fact and/or technical reasoning to reasonably support the determination that the allegedly inherent characteristic necessarily flows from the teachings of the applied prior art." See MPEP §2112 (IV)(emphasis in original).

Further, Applicants note that inherency "may not be established by probabilities or possibilities. The mere fact that a certain thing may result from a given set of circumstances is not sufficient." MPEP §2112 (IV) (emphasis added).

Applicants submit that the Examiner has not come forward with any factual basis as to why the functional features recited in claim 14 must necessarily be present in the cited prior art. Accordingly, Applicants submit that claim 14 is patentable over the cited prior art and respectfully request that the rejection be reconsidered and withdrawn.

Regarding claims 15-19, Applicants note that these claims depend from claim 14 and are therefore considered patentable at least by virtue of their dependency.

B. Claims 20 and 21

Regarding claim 20, Applicants note that this claim is a **method claim** which recites similar features as set forth above in claim 14 (which is an apparatus claim).

As explained above, the Examiner has not given patentable weight to the functional language recited in claim 14 because the Examiner believes that functional limitations in an

apparatus claim should not be entitled to patentable weight (which is traversed by Applicants for the reasons set forth above).

With respect to the rejection of method claim 20, however, Applicants note that the Examiner has merely grouped the rejection of this claim together with the rejection of claim 14, without addressing the specific language set forth in the **steps** recited in claim 20. Applicants respectfully submit that this is clearly improper, and request that the Examiner issue a new Office Action specifically addressing all of the features set forth in method claim 20.

Applicants respectfully submit that Hori and Ginter do not teach or suggest all of the features set forth in claim 20. For example, Applicants note that Hori and Ginter do not teach or suggest at least the feature recited in claim 20 of a digital signature management step, being performed by the digital signature management unit, of (i) generating a hash value of the encrypted license information before the encrypted license information is stored into the storage unit, and storing the generated hash value into a built-in memory, (ii) reading the encrypted license information stored in the storage unit, generating a hash value of the read encrypted license information, and comparing the hash value stored in the built-in memory with the generated hash value of the read encrypted license information, with a result of the comparison being used to verify validity of the read encrypted license information, the validity indicating that the read encrypted license information has not been tampered with.

In particular, with respect to Hori, Applicants note that this reference discloses the use of a controller 1420 in a memory card 110, wherein the controller has the ability to generate a hash value, and to encrypt the generated hash value (see paragraph [0223]). In this regard, however, Applicants note that the hash value of Hori is merely a hash value of status information (i.e., information in which a status flag is added to a reception log) (see paragraphs [0219]

through [0222]), and therefore, is clearly not a hash value of encrypted license information as recited in claim 20.

In addition, as explained in Hori, a decryption process is performed on the encrypted hash value to obtain a signature data hash corresponding to the encrypted data, and then authenticity of the status information is checked based on the encrypted status and the signature data (see paragraph [0027]). Thus, while Hori discloses the ability to determine the authenticity of the status information based on the encrypted status information and the signature data, Applicants respectfully submit that this aspect of Hori clearly does not correspond to the feature recited in claim 20 of comparing the hash value stored in the built-in memory with the generated hash value of the read encrypted license information.

Based on the foregoing, Applicants note that while Hori discloses the ability to generate a hash value of status information, and to determine the authenticity of the status information based on the encrypted status information and the signature data, that Hori does not disclose or in any way suggest the above-noted feature recited in claim 20 of (i) generating a hash value of the encrypted license information before the encrypted license information is stored into the storage unit, and storing the generated hash value into a built-in memory, (ii) reading the encrypted license information stored in the storage unit, generating a hash value of the read encrypted license information, and comparing the hash value stored in the built-in memory with the generated hash value of the read encrypted license information, with a result of the comparison being used to verify validity of the read encrypted license information, the validity indicating that the read encrypted license information has not been tampered with.

Further, Applicants respectfully submit that Ginter fails to cure the above-noted deficiencies of Hori. Accordingly, Applicants respectfully submit that claim 20 is patentable over the cited prior art, an indication of which is kindly requested.

Regarding claim 21, Applicants note that this claim recites the feature of (i) generating a hash value of the encrypted license information before the encrypted license information is stored into the storage unit, and storing the generated hash value into a built-in memory, (ii) reading the encrypted license information stored in the storage unit, generating a hash value of the read encrypted license information, and comparing the hash value stored in the built-in memory with the generated hash value of the read encrypted license information, with a result of the comparison being used to verify validity of the read encrypted license information, the validity indicating that the read encrypted license information has not been tampered with.

For at least similar reasons as discussed above with respect to claim 20, Applicants respectfully submit that Hori and Ginter do not teach, suggest or otherwise render obvious at least the above-noted feature recited in claim 21. Accordingly, Applicants submit that claim 21 is patentable over the cited prior art, an indication of which is kindly requested.

III. Conclusion

In view of the above, reconsideration and allowance of this application are now believed to be in order, and such actions are hereby solicited.

If any points remain in issue which the Examiner feels may best be resolved through a personal or telephone interview, the Examiner is kindly requested to contact the undersigned at the telephone number listed below.

Respectfully submitted,

Motoji OHMORI et al.

/Kenneth W. Fields/
2010.05.17 13:28:42 -04'00'

By _____
Kenneth W. Fields
Registration No. 52,430
Attorney for Applicants

KWF/krg
Washington, D.C. 20005-1503
Telephone (202) 721-8200
Facsimile (202) 721-8250
May 17, 2010